

①

Corrigé de l'examen final du 31 mai 2021

Ex 1.

- 1) On a  $145 = 5 \times 29$  et  $55 = 5 \times 11$  donc  $\text{pgcd}(145, 55) = 5$ .
- 2) Puisque  $5 \mid 145x + 55y$  et que  $5 \nmid 237$ , l'équation  $145x + 55y = 237$  n'admet pas de solutions dans  $\mathbb{Z}$ .

L'équation  $145x + 55y = 237$  se simplifie à l'équation équivalente  $29x + 11y = 5$  que nous allons résoudre en pensant par une solution particulière  $(x_0, y_0)$ . Pour cela cherchons des coefficients de Bézout pour 29 et 11 via l'algorithme d'Euclid :

$$29 = 2 \times 11 + 7, \quad 11 = 7 + 4, \quad 7 = 4 + 3, \quad 4 = 3 + 1$$

$$\begin{aligned} \text{Par conséquent } 1 &= 4 - 3 = 4 - (7 - 4) = 2 \times 4 - 7 = 2(11 - 7) - 7 = \\ &= 2 \times 11 - 3 \times 7 = 2 \times 11 - 3(29 - 2 \times 11) = 8 \times 11 - 3 \times 29 \end{aligned}$$

$$\text{d'où } -3 \times 29 + 8 \times 11 = 1 \Leftrightarrow 29 \times (-15) + 11 \times (40) = 5$$

une solution particulière et alors  $x_0 = -15, y_0 = 40$ .

$$\text{On obtient } 29x + 11y = 29x_0 + 11y_0 \Leftrightarrow 29(x - x_0) = 11(y_0 - y)$$

Or  $11 \mid 29(x - x_0)$  et  $\text{pgcd}(11, 29) = 1$  donc d'après le lemme de Gauss  $11 \mid x - x_0$ , c'est à dire  $x - x_0 = 11k$  avec  $k \in \mathbb{Z}$

$$\text{Cela implique } 29 \times 11k = 11(y_0 - y) \Leftrightarrow y_0 - y = 29k$$

(2)  $y = y_0 - 29k$ . Les solutions générales sont de la forme

$$x = 11k + x_0 = 11k - 15, \quad y = y_0 - 29k = 40 - 29k$$

avec  $k \in \mathbb{Z}$ .

$$\begin{aligned} \text{Vérification : } 29(11k - 15) + 11(40 - 29k) &= \\ &= 29 \times 11k - 29 \times 15 + 11 \cdot 40 - 11 \times 29k = \\ &= 29 \times 15 + 11 \times 40 = 5 \end{aligned}$$

3) On cherche d'abord un inverse  $a$  pour 2 modulo 55 pour transformer l'équation  $2x \equiv 1 \pmod{55}$  en une équation du type  $x \equiv a \pmod{55}$

Or  $55 - 2 \times 27 = 1$  donc  $a = -27$  est un inverse de 2 modulo 55.

Par conséquent  $(-27)2x \equiv -27 \pmod{55} \Leftrightarrow x \equiv -27 \pmod{55}$   
 $\Leftrightarrow x \equiv 28 \pmod{55}$ .

Notre système devient  $S \left\{ \begin{array}{l} x \equiv 3 \pmod{145} \\ x \equiv 28 \pmod{55} \end{array} \right.$  et ne admet des

solutions car  $\text{pgcd}(145, 55) = 5 \mid 28 - 3 = 25$ . Pour le trouver revenons à la relation de Bézout trouvée à la question 2:

$$29 \times (-15) + 11 \times 40 = 5 \quad \Leftrightarrow \quad 29 \times (-15) + 11 \times 8 = 1$$

Elle nous permet de trouver une solution particulière pour le système  $S'$   $\left\{ \begin{array}{l} x \equiv 3 \pmod{29} \\ x \equiv 28 \pmod{11} \end{array} \right.$  en remarquant que

$$\left\{ \begin{array}{l} 11 \times 8 \equiv 1 \pmod{29} \\ 11 \times 8 \equiv 0 \pmod{11} \end{array} \right. + \left\{ \begin{array}{l} 29 \times (-3) \equiv 0 \pmod{29} \\ 29 \times (-3) \equiv 1 \pmod{11} \end{array} \right. \text{ et donc que}$$

$$x_0 = 11 \times 8 \times 3 + (29) \times (-3) \times 28 \quad \text{vérifie} \quad \left\{ \begin{array}{l} x_0 \equiv 3 \pmod{29} \\ x_0 \equiv 28 \pmod{11} \end{array} \right.$$

Il se trouve que  $x_0$  est aussi solution particulière de  $S$ .

$$\text{En effet } \left\{ \begin{array}{l} x_0 \equiv 3 \pmod{145} \\ x_0 \equiv 28 \pmod{55} \end{array} \right. \text{ alors } \left\{ \begin{array}{l} x \equiv x_0 \pmod{145} \\ x \equiv x_0 \pmod{55} \end{array} \right. \quad (\Rightarrow)$$

$$\left\{ \begin{array}{l} x - x_0 \equiv 0 \pmod{145} \\ x - x_0 \equiv 0 \pmod{55} \end{array} \right. \quad (\Rightarrow) \quad \left\{ \begin{array}{l} 145 \mid x - x_0 \\ 55 \mid x - x_0 \end{array} \right. \quad (\Rightarrow) \quad \text{ppcm}(145, 55) \mid x - x_0 \\ \Rightarrow 1595 \mid x - x_0.$$

$$\Rightarrow x \equiv x_0 \pmod{1595} \quad (\Rightarrow) \quad x \equiv -2172 \pmod{1595} \quad (\Rightarrow) \quad x \equiv 1018 \pmod{1595}$$

Vérification: on a bien  $\left\{ \begin{array}{l} 1018 \equiv 3 \pmod{145} \\ 1018 \equiv 28 \pmod{55} \end{array} \right.$  et  $2036 \equiv 1 \pmod{55}$ .

Ex 2.

q1) On a  $2^0 \equiv 1 \pmod{5}$ ,  $2^1 \equiv 2 \pmod{5}$ ,  $2^2 \equiv -1 \pmod{5}$ ,  $2^3 \equiv -2 \pmod{5}$ ,  $2^4 \equiv 1 \pmod{5}$

donc  $2^{4k} \equiv (2^4)^k \equiv 1 \pmod{5}$ ,  $2^{4k+1} \equiv 2^{4k} \cdot 2 \equiv 2 \pmod{5}$ ,  $2^{4k+2} \equiv 2^{4k} \cdot 2^2 \equiv -1 \pmod{5}$

et  $2^{4k+3} \equiv 2^{4k} \cdot 2^3 \equiv -2 \equiv 3 \pmod{5}$ , pour  $k \in \mathbb{Z}$

Par conséquent si  $n = 4k$ ,  $2^n \equiv 1 \pmod{5}$ , 1 est le reste cherché

si  $n = 4k+1$ ,  $2^n \equiv 2 \pmod{5}$ , 2 est le reste cherché

si  $n = 4k+2$ ,  $2^n \equiv -1 \pmod{5}$ , 4 est le reste cherché

et enfin si  $n = 4k+3$ ,  $2^n \equiv 3 \pmod{5}$ , 3 est le reste cherché, pour  $k \in \mathbb{Z}$ .

q2) On a  $10 \equiv -1 \pmod{11}$  donc  $10^{13} \equiv (-1)^{13} \equiv -1 \pmod{11}$   
 $\equiv 10 \pmod{11}$

et 10 est le reste de la division euclidienne de  $10^{13}$  par 11.

Ex 3.

q1) On a  $\langle \bar{k} \rangle = \mathbb{Z}/6\mathbb{Z}$  et  $\text{pgcd}(k, 6) = 1$  donc les générateurs de  $\mathbb{Z}/6\mathbb{Z}$  sont  $\bar{1}$  et  $\bar{5}$ , qui sont également les éléments inversibles pour la multiplication dans l'anneau  $(\mathbb{Z}/6\mathbb{Z}, +, \times)$ .

(Ils seront donc aussi la q3) car  $(\mathbb{Z}/6\mathbb{Z}, \times) = \{\bar{1}, \bar{5}\}$  est cyclique engendré par  $\bar{5}$ .  
En effet  $\bar{5}^2 = \bar{1}$  dans  $\mathbb{Z}/6\mathbb{Z}$ .

q2) Si un morphisme  $f: \mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$  vérifie  $f(\bar{1}) = \bar{1}$ , il doit vérifier aussi  $f(\bar{1} + \bar{1} + \bar{1}) = f(\bar{1}) + f(\bar{1}) + f(\bar{1}) = \bar{1} + \bar{1} + \bar{1} = \bar{3}$

Or  $\bar{3} = \bar{0}$  dans  $\mathbb{Z}/3\mathbb{Z}$  et  $f(\bar{0}) = \bar{0} + \bar{3}$  dans  $\mathbb{Z}/6\mathbb{Z}$

Il n'y a donc pas de morphisme  $f$  tel que  $f(\bar{1}) = \bar{1}$ .

Par contre si  $f(\bar{1}) = \bar{2}$  on a bien  $f(3 \cdot \bar{1}) = 3 \cdot \bar{2}$  car  $3 \cdot \bar{2} = \bar{6} = \bar{0}$  dans  $\mathbb{Z}/6\mathbb{Z}$ . Et en posant  $f(\bar{k}) = \bar{2k}$  on a  $f$  application bien définie

de  $\mathbb{Z}/3\mathbb{Z}$  dans  $\mathbb{Z}/6\mathbb{Z}$  car  $f(\bar{k} + 3\bar{l}) = \overline{2(k + 3l)} = \overline{2k + 6l} = \overline{2k} = f(\bar{k})$

pour  $k, l \in \mathbb{Z}$ . Cette condition doit être vérifiée car  $\overline{k + 3l} = \bar{k}$ .

Cette application est un morphisme (car  $f(\bar{k}_1 + \bar{k}_2) = f(\bar{k}_1 + \bar{k}_2) = \overline{2(k_1 + k_2)} = \overline{2k_1 + 2k_2} = f(\bar{k}_1) + f(\bar{k}_2)$ , et  $f$  est injectif car  $\overline{k} = \bar{k} \in \mathbb{Z}/3\mathbb{Z} \mid \bar{k} \neq \bar{0}$  dans  $\mathbb{Z}/6\mathbb{Z} \} = \{\bar{1}\} \cap \{2k\} = \{\bar{2}\} \mid 3k \neq \bar{0} \}. Mais f n'est pas surjectif car  $\text{Im } f = \{\bar{2}, \bar{4}, \bar{0}\} \neq \mathbb{Z}/6\mathbb{Z}$ .$

Ex4. On a  $\tau = (125)(34)$  et  $\varepsilon(\tau) = \varepsilon((125))\varepsilon((34)) = (-1)^{3-1}(-1)^{2-1} = -1$ .

Ex5. q1) Il faut choisir 2 blancs parmi 7 et 3 noirs parmi 10.

On a  $C_7^2$  choix pour les 2 blancs et  $C_{10}^3$  choix pour les 3 noirs donc il y a  $C_7^2 \cdot C_{10}^3$  tirages contenant 2 blancs et 3 noirs.

q2) Si  $A = \text{"5 blancs"}$  on a  $\#A = C_7^5$  et pour

$\Omega = \text{"5 chocolats"}$  on a  $\#\Omega = C_{17}^5$  donc

$$P(A) = \frac{C_7^5}{C_{17}^5}$$

q3) Si  $B = \text{"au moins un chocolat noir"}$  alors  $B = \bar{A}$  donc

$$P(B) = 1 - P(A) = 1 - C_7^5 / C_{17}^5.$$

q4) Si  $C = \text{"noir au premier tirage"}$  et  $D = \text{"noir au second tirage"}$

alors  $P(C) = \frac{10}{17}$  et  $P(D) = P(D \cap C) + P(D \cap \bar{C}) = P(C)P(D/C) + P(\bar{C})P(D/\bar{C})$

$$= \frac{10}{17} \cdot \frac{9}{16} + \frac{7}{17} \cdot \frac{10}{16} = \frac{10}{17} \quad \text{car après un premier tirage noir}$$

il reste 16 chocolats dont 9 noirs et après un premier tirage blanc

il reste 16 chocolats dont 10 noirs. On voit que  $P(D) = P(C)$  donc c'est pareil de tirer un noir au premier ou au second tirage.

En effet pour un univers  $\Omega = \{(a, b) \mid a, b \in \{N_i, B_j \mid i \in [1, 10]\} \cup j \in [1, 7]\}$

qui prend en compte toutes les possibilités (équiprobales)

de couples d'issues (premier tirage, second tirage) il y a autant

de couples avec  $N_i$  en première composante que de couples avec

$N_i$  en seconde composante. Donc  $\#C = 10 \times 16 = \#D = 16 \times 10$

et  $\#\Omega = 17 \times 16$  choix second  
choix 1<sup>er</sup> comp

choix 1<sup>er</sup> comp  
première composante choix 2<sup>nd</sup> comp  
seconde composante

$$\text{et } P(C) = P(D) = \frac{10 \times 16}{17 \times 16} = \frac{10}{17}.$$

Les chocolats noirs ont été numérotés  $N_1, N_2, \dots, N_{10}$  et les

chocolats blancs ont été numérotés  $B_1, B_2, \dots, B_7$ , bien sûr.

Ex6.

On remarque que  $x \neq e$  tel que  $x^2 = e$  signifie exactement  $\text{ord}(x) = 2$ , et cela signifie encore que  $x = x^{-1}$ .  
 Donc si  $G$  ne contient pas d'élément d'ordre 2, on aura  $\forall x \in G \setminus \{e\}$  que  $x \neq x^{-1}$ . On peut alors regrouper les éléments de  $G \setminus \{e\}$  en couples  $(x, x^{-1})$  jusqu'à épuisement des éléments de  $G \setminus \{e\}$  c'est à dire  $G \setminus \{e\} = \{ \underbrace{\{x_1, x_1^{-1}\}}, \dots, \underbrace{\{x_k, x_k^{-1}\}} \}$  pour  $k \in \mathbb{N}^*$

Ceci entraîne  $|G| = 1 + 2k$  ce qui contredit l'hypothèse. Par conséquent il existe au moins un élément  $x$  de  $G$  d'ordre 2. On constate que  $|\{x \in G, \text{ord}(x) = 2\}|$  est en effet un nombre impair.

Ex7. Puisque  $p$  et  $q$  sont impairs on sait que  $N$  est pair donc  $N$  admet au moins 2 diviseurs : 2 et  $\frac{N}{2}$ .

Or  $\frac{N}{2} = \frac{p+q}{2}$  est strictement compris entre  $p$  et  $q$ , qui sont des nombres premiers consécutifs.

Donc  $\frac{N}{2}$  ne peut pas être premier, il se décompose en un produit  $n_1 \cdot n_2$  avec  $n_1, n_2 \neq 1$

Cela implique que  $N = 2 \cdot n_1 \cdot n_2$  donc que  $N$  a au moins trois diviseurs propres 2,  $n_1$  et  $n_2$ .